Managing Enterprise Risk

FISMA Lessons Learned and Implementation Tips

February 23, 2007

Dr. Ron Ross

Computer Security Division

Information Technology Laboratory

Current State of Affairs

- Continuing serious attacks on federal information systems, large and small; targeting key federal operations and assets.
- Significant exfiltration of critical and sensitive information and implantation of malicious software.
- Attacks are organized, disciplined, aggressive, and well resourced; many are extremely sophisticated.
- Adversaries: nation states, terrorist groups, hackers, criminals, and any individuals or groups with intentions of compromising a federal information system.
- Increasing number of trusted employees taking dangerous and imprudent actions with respect to organizational information systems.

FISMA Strategic Vision

- We are building a solid foundation of information security across one of the largest information technology infrastructures in the world based on comprehensive security standards and technical guidance.
- We are institutionalizing a comprehensive Risk Management Framework that promotes flexible, cost-effective information security programs for federal agencies.
- We are establishing a fundamental level of “security due diligence” for federal agencies and their contractors based on minimum security requirements and security controls.

Key Players

- Authorizing Officials
- Mission / Information System Owners
- Chief Information Officer
- Chief Information Security Officers
- Inspectors General

FISMA Characteristics

- The NIST *Risk Management Framework* and the associated security *standards* and *guidance* documents provide a process that is:
  - Disciplined
  - Flexible
  - Extensible
  - Repeatable
  - Organized
  - Structured

"Building information security into the infrastructure of the organization… so that critical enterprise missions and business cases will be protected."

Managing Enterprise Risk

- Key activities in managing enterprise-level risk—risk to the enterprise and to other organizations resulting from the operation of an information system:
  - ✓ Categorize the information system (criticality/sensitivity)
  - ✓ Select and tailor baseline (minimum) security controls
  - ✓ Supplement the security controls based on risk assessment
  - ✓ Document security controls in system security plan
  - ✓ Implement the security controls in the information system
  - ✓ Assess the security controls for effectiveness
  - ✓ Authorize information system operation based on mission risk
  - ✓ Monitor security controls on a continuous basis

Risk Management Framework

Starting Point

FIPS 199 / SP 800-60

CATEGORIZE
Information System

Define criticality /sensitivity of information system according to potential impact of loss

FIPS 200 / SP 800-53

SELECT
Security Controls

Select baseline (minimum) security controls to protect the information system; apply tailoring guidance as appropriate

SP 800-53 / SP 800-30

SUPPLEMENT
Security Controls

Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

SP 800-18

DOCUMENT
Security Controls

Document in the security plan, the security requirements for the information system and the security controls planned or in place

SP 800-70

IMPLEMENT
Security Controls

Implement security controls; apply security configuration settings

SP 800-53A

ASSESS
Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)

SP 800-37

AUTHORIZE
Information System

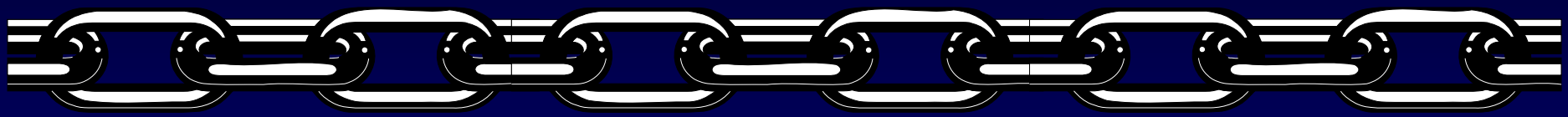
Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

SP 800-37 / SP 800-53A

MONITOR
Security Controls

Continuously track changes to the information system that may affect security controls and reassess control effectiveness

Information Security Program



Links in the Security Chain: Management, Operational, and Technical Controls

- ✓ Risk assessment
- ✓ Security planning
- ✓ Security policies and procedures
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Security in acquisitions
- ✓ Physical security
- ✓ Personnel security
- ✓ Security assessments
- ✓ Certification and accreditation
- ✓ Access control mechanisms
- ✓ Identification & authentication mechanisms (Biometrics, tokens, passwords)
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Boundary and network protection devices (Firewalls, guards, routers, gateways)
- ✓ Intrusion protection/detection systems
- ✓ Security configuration settings
- ✓ Anti-viral, anti-spyware, anti-spam software
- ✓ Smart cards

Adversaries attack the weakest link…where is yours?

Information Security Strategy

- Successful FISMA implementation demands that organizations adopt an *enterprise-wide* security strategy.
- Metrics of a successful implementation:
  - Cost-effective
  - Consistent
  - Comprehensive
  - Effective

Six Essential Activities

- FIPS 199 security categorizations
- Identification of common controls
- Application of tailoring guidance for FIPS 200 and SP 800-53 security controls
- Effective strategies for continuous monitoring of security controls (assessments)
- Security controls in external environments
- Use restrictions

Security Categorization

- The most important step in the Risk Management Framework.
- Affects all other steps in the framework from selection of security controls to level of effort in assessing control effectiveness.
- Expect the distribution of categorized federal information systems to look like a normal or Bell-curve centered on moderate-impact.

Security Categorization

- Important change in SP 800-53, Revision 1, security control RA-2.
- FIPS 199 security categorizations consider both agency and national impacts.
- New language:

  "The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system."

FISMA Implementation Tip #1

Strategy for successful implementation—

- Conduct FIPS 199 *impact analyses* as a corporate-wide exercise with the participation of key officials (e.g., Chief Information Officer, Senior Agency Information Security Officer, Authorizing Officials, Mission/System Owners).

  Rationale: The agency is heavily dependent upon its information systems and information technology infrastructure to successfully conduct critical missions. Therefore, the protection of those critical missions is of the highest priority. An incorrect information system impact analysis (i.e., incorrect FIPS 199 security categorization) results in the agency either over protecting the information system and wasting valuable security resources or under protecting the information system and placing important operations and assets at risk.

Common Controls

- Categorize all information systems first, enterprise-wide.
- Select common controls for all similarly categorized information systems (low, moderate, high impact).
- Be aggressive; when in doubt, assign a common control.
- Assign responsibility for common control development, implementation, assessment, and tracking (or documentation of where employed).

Common Controls

- Ensure common control-related information (e.g., assessment results) is shared with all information system owners.
- In a similar manner to information systems, common controls must be continuously monitored with results shared with all information system owners.
- Information system owners must supplement the common portion of the security control with system specific controls as needed to complete security control coverage.

Common Controls

- The more common controls an organization identifies, the greater the cost savings and consistency of security capability during implementation.
- Common controls can be assessed by organizational officials (other than the information system owner), thus taking responsibility for effective security control implementation.

FISMA Implementation Tip #2

Strategy for successful implementation—

- Conduct the selection of *common security controls* (i.e., agency infrastructure-related controls or controls for common hardware/software platforms) as a corporate-wide exercise with the participation of key officials (e.g., Chief Information Officer, Senior Agency Information Security Officer, Authorizing Officials, System Owners).

  Rationale: The careful selection of common security controls can save the agency significant resources and facilitate a more consistent application of security controls enterprise-wide. Agency officials must assign responsibility for the development, implementation, assessment, and tracking of the controls and ensure that the resulting information is available to all interested parties.

Tailoring Guidance

- FIPS 200 and SP 800-53 provide significant flexibility in the security control selection and specification process—if organizations choose to use it.
- Includes:
  - Scoping guidance;
  - Compensating security controls; and
  - Organization-defined security control parameters.

Scoping Guidance I

- Common security control-related considerations

  Common controls are managed by an organizational entity other than the information system owner. Organizational decisions on which security controls are viewed as common controls may greatly affect the responsibilities of individual information system owners.

- Operational/environmental-related considerations

  Security controls that are dependent on the nature of the operational environment are applicable only if the information system is employed in an environment necessitating the controls.

Scoping Guidance II

- Physical Infrastructure-related considerations

  Security controls that refer to organizational facilities (e.g., physical controls such as locks and guards, environmental controls for temperature, humidity, lighting, fire, and power) are applicable only to those sections of the facilities that directly provide protection to, support for, or are related to the information system.

- Public access-related considerations

  Security controls associated with public access information systems should be carefully considered and applied with discretion since some security controls from the specified control baselines (e.g., identification and authentication, personnel security controls) may not be applicable to users accessing information systems through public interfaces.

Scoping Guidance III

- Technology-related considerations
  - Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) are applicable only if those technologies are employed or are required to be employed within the information system.
  - Security controls are applicable only to the components of the information system that provide or support the security capability addressed by the control and are sources of potential risk being mitigated by the control.
  - Security controls that can be either explicitly or implicitly supported by automated mechanisms, do not require the development of such mechanisms if the mechanisms do not already exist or are not readily available in commercial or government off-the-shelf products.

Scoping Guidance IV

- Policy/regulatory-related considerations

  Security controls that address matters governed by applicable laws, Executive Orders, directives, policies, standards, or regulations (e.g., privacy impact assessments) are required only if the employment of those controls is consistent with the types of information and information systems covered by the applicable laws, Executive Orders, directives, policies, standards, or regulations.

Scoping Guidance V

- Scalability-related considerations

  Security controls are scalable with regard to the extent and rigor of the control implementation. Scalability is guided by the FIPS 199 security categorization of the information system being protected.

- Security objective-related considerations

  Security controls that uniquely support the confidentiality, integrity, or availability security objectives may be downgraded to the corresponding control in a lower baseline (or appropriately modified or eliminated if not defined in a lower baseline) if, and only if, the downgrading action: (i) is consistent with the FIPS 199 security categorization before moving to the high water mark; (ii) is supported by an organizational assessment of risk; and (iii) does not affect the security-relevant information within the information system.

Compensating Security Controls

- A compensating security control is a management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provides equivalent or comparable protection for an information system.
- Mission-driven considerations may require alternate solutions (e.g., AC-11 session lock not advisable in certain systems).

Compensating Security Controls

- The organization selects a compensating control from NIST SP 800-53, or if an appropriate compensating control is not available in the security control catalog, the organization adopts a suitable compensating control;
- The organization provides a complete and convincing rationale for how the compensating control provides an equivalent security capability or level of protection for the information system and why the related baseline security control could not be employed; and
- The organization assesses and formally accepts the risk associated with employing the compensating control in the information system.

Organization-defined Parameters

- Security controls containing organization-defined parameters (i.e., assignment and/or selection operations) give organizations the flexibility to define selected portions of the controls- to support specific organizational requirements or objectives.

CP-9 INFORMATION SYSTEM BACKUP

Control: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [*Assignment: organization-defined frequency*] and protects backup information at the storage location.

FISMA Implementation Tip #3

Strategy for successful implementation—

- For each security control baseline (low, moderate, or high) identified in NIST Special Publication 800-53, apply the ***tailoring guidance*** to modify the set of controls to meet the specific operational requirements of the agency.

  Rationale: Application of the tailoring guidance in Special Publication 800-53 can eliminate unnecessary security controls, incorporate compensating controls when needed, and specify agency-specific parameters. Tailoring activities and associated tailoring decisions should be well documented with appropriate justification capable of providing reasoned arguments to auditors.

FISMA Implementation Tip #4

Strategy for successful implementation—

- For each tailored security control baseline, *supplement* the security controls with additional controls and/or control enhancements based on the results of an organizational assessment of risk.

Rationale: The tailored baseline represents the starting point for determining the needed level of security *due diligence* to be demonstrated by an organization toward the protection of its operations and assets. In many cases, additional security controls or control enhancements will be needed to address specific threats to and vulnerabilities in an information system or to satisfy the requirements of applicable laws, Executive Orders, directives, policies, standards, or regulations.

Continuous Monitoring

- Transforming certification and accreditation from a static to a *dynamic* process.
- Strategy for *monitoring* selected security controls; which controls selected and how often assessed.
- Control selection driven by *volatility* and *Plan of Action and Milestones (POAM).*
- Facilitates annual FISMA *reporting* requirements.

External Service Providers

- Organizations are becoming increasingly reliant on information system services provided by external service providers to carry out important missions and functions.
- External information system services are services that are implemented outside of the system's accreditation boundary (i.e., services that are used by, but not a part of, the organizational information system).
- Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges.

External Service Providers

- Organizations have varying degrees of control over external service providers.
- Organizations must establish trust relationships with external service providers to ensure the necessary security controls are in place and are effective in their application.
- Where control of external service providers is limited or infeasible, the organization factors that situation into its risk assessment.

Information System Use Restrictions

- A method to reduce or mitigate risk, for example, when:
  - Security controls cannot be implemented within technology and resource constraints; or
  - Security controls lack reasonable expectation of effectiveness against identified threat sources.
- Restrictions on the use of an information system are sometimes the only prudent or practical course of action to enable mission accomplishment in the face of determined adversaries.

Compliance Schedule

NIST Security Standards and Guidelines

- For legacy information systems, agencies are expected to be in compliance with NIST security standards and guidelines within one year of the publication date unless otherwise directed by OMB or NIST.*
- For information systems under development, agencies are expected to be in compliance with NIST security standards and guidelines immediately upon deployment of the system.

*The one-year compliance date for revisions to NIST Special Publications applies only to the new and/or updated material in the publications resulting from the periodic revision process. Agencies are expected to be in compliance with previous versions of NIST Special Publications within one year of the publication date of the previous versions.

Compliance

NIST Standards and Guidelines

- While agencies are required to follow NIST *guidance* in accordance with OMB policy, there is flexibility in how agencies apply the guidance.
- Unless otherwise specified by OMB, the 800-series guidance documents published by NIST generally allow agencies some *latitude* in their application.
- Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of *adequate security* for federal information systems.

Compliance

NIST 800-Series Guidelines

- When assessing agency compliance with NIST guidance, auditors, evaluators, and/or assessors should consider:
  - The intent of the security concepts and principles articulated within the particular guidance document; and
  - How the agency applied the guidance in the context of its specific mission responsibilities, operational environments, and unique organizational conditions.

Myth Versus Reality

- MYTH: The FISMA security standards and guidance have eliminated the need for or use of the risk assessment for the information system.
- REALITY: The risk assessment is still a required step in the NIST Risk Management Framework to determine the additional security controls for the information system after tailoring the baseline controls in order to adequately mitigate risk.

Some Final Thoughts

- Your adversaries don't care about FISMA compliance—they just want to compromise your information systems.
- FISMA is not just a paperwork exercise; it is the application of real security controls to federal information systems that are supporting critical federal missions.

Some Final Thoughts

- The most dangerous person to an enterprise is an uninformed authorizing official.
- FISMA security standards and guidance should not drive the mission; rather the standards and guidance should support the mission.

Some Final Thoughts

- FISMA is about the application of common sense security—it is not dogma to be followed blindly.
- The only mandatory requirement under the FISMA security standards and guidance is the application of the NIST Risk Management Framework—everything else is negotiable.

Some Final Thoughts

- Policies and procedures are not just FISMA paperwork—they are a corporate statement of commitment to protecting critical enterprise information and information systems and the necessary details describing how to do it.

Some Final Thoughts

- If the successful accomplishment of enterprise missions depends on information systems, including the information processed, stored, and transmitted by those systems, the systems must be dependable. To be dependable in the face of serious threats, the systems must be appropriately protected.

Some Final Thoughts

- *Never underestimate the capabilities of your adversaries.*
- *Never overestimate the ability of your organization and your personnel to protect critical enterprise missions.*
- *Information technology—if you can't protect it, don't deploy it.*

Key Standards and Guidelines

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Management)
- NIST Special Publication 800-37 (Certification & Accreditation)
- NIST Special Publication 800-53 (Recommended Security Controls)
- NIST Special Publication 800-53A (Security Control Assessment)
- NIST Special Publication 800-59 (National Security Systems)
- NIST Special Publication 800-60 (Security Category Mapping)

Many other FIPS and NIST Special Publications provide security standards and guidance supporting the FISMA legislation…

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leader

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Matt Scholl
(301) 975-2941
matthew.scholl@nist.gov

Information and Feedback
Web: csrc.nist.gov/sec-cert
Comments: sec-cert@nist.gov